Carlos F. Osorio (*pro hac vice admission pending*)
Florida Bar No. 597546
cosorio@osorioint.com
W. Daniel Zafutto (*pro hac vice admission pending*)
Florida Bar No. 743461
dzafutto@osorioint.com
Andres F. Rey (*pro hac vice admission pending*)
Florida Bar No. 118875
arey@osorioint.com
OSORIO INTERNACIONAL, P.A.
175 S.W. 7 Street, Suite 1900
Miami, FL 33130
Tel: 305-900-4103

George J. Vila (*pro hac vice admission pending*)
Florida Bar No. 141704
gvila@gjvpa.com
GEORGE J. VILA, P.A.
201 Alhambra Circle, Suite 702
Coral Gables, FL 33134-5111
Tel: 305-445-2540

Monte S. Travis (CA Bar No. 84032)
montetravis@mac.com
Robert P. Travis (CA Bar No. 182667)
robert.p.travis@icloud.com
TRAVIS & TRAVIS
1160 Battery Street East, Suite 100
San Francisco, CA 94111-1231
Tel: 415-939-0576

Attorneys for Plaintiff
Francesco Corallo

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FRANCESCO CORALLO,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED, Q CYBER TECHNOLOGIES LIMITED, and APPLE, INC.,

Defendants.

Case No. _____

COMPLAINT

DEMAND FOR JURY TRIAL

COMPLAINT

Plaintiff FRANCESCO CORALLO ("**Corallo**") sues Defendants NSO GROUP TECHNOLOGIES LIMITED ("**NSO**") and Q CYBER TECHNOLOGIES LIMITED ("**Q Cyber**") (collectively the "**NSO Defendants**"), and APPLE, INC. ("**Apple**") (collectively "**Defendants**"), and alleges as follows:

NATURE OF THE CASE

1. Plaintiff brings this action for damages and injunctive relief pursuant to the Alien Tort Claims Act, 28 U.S.C. § 1350, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and for California state law claims for invasion of privacy, civil conspiracy, negligence, California's Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, California's False Advertising Law, Cal. Bus. and Prof. Code, §§ 17500, *et seq.,* and intentional inflict of emotional distress.

2. In particular, this action seeks redress for NSO Defendants' torts in violation of the law of nations and international law from their systematic abuse of human rights, targeting, harassment, persecution, intentional infliction of emotional distress, invasion of privacy, as well as other offensive and actionable conduct.

3. This action also raises claims for violations of federal and state law arising out of the NSO Defendants' egregious, deliberate, and intentional hacking of Corallo's Apple iPhone device and iCloud account through the use of surveillance technology or "spyware,"[1] including NSO Defendants' Pegasus spyware and FORCEDENTRY security exploit (used to deploy NSO Defendants' Pegasus spyware onto the Apple user's devices).

4. Such hacking has been confirmed by expert, forensic analysis involving a review of the affected iPhone device.

5. This action also seeks redress for Apple's negligence in failing to (1) warn (2)

[1] "Malware, short for 'malicious software,' includes viruses and spyware that can steal personal information, send spam, and commit fraud. . . . Spyware is one type of malware that can monitor or control your computer use. It may be used to send consumers pop-up ads, redirect their computers to unwanted websites, monitor their Internet surfing, or record their keystrokes, which, in turn, could lead to identity theft." https://www.ftc.gov/news-events/topics/identity-theft/spyware-malware.

prevent and/or (3) adequately and reasonably defend against the hacking by NSO Defendants despite Apple's knowledge that NSO Defendants were actively targeting its customers with their malware and spyware and other surveillance technology, and for falsely advertising its ability to prevent such cyberattacks.

6. Corallo (through his various business entities) is a successful businessman with business interests in the island of Sint Martin (a Netherlands/French West Indies Territory), other Caribbean territories, as well as Italy. As set forth herein, upon information and belief, the Governments of The Netherlands and/or Italy, for political purposes, have targeted Plaintiff and have hired or conspired with NSO Defendants to violate Plaintiff's human rights and commit tortious acts against him, through acts of harassment, persecution, intentional infliction of emotional distress, invasion of privacy, as well as other offensive and actionable conduct.

7. Forensic analysis has confirmed that such abusive conduct and harassment included the illegal recording, surveillance and data theft of Corallo, his family, his various businesses, business associates and attorneys.

PARTIES

8. Corallo is an individual, native of Italy and a naturalized citizen of The Netherlands, who currently resides in Sint Maarten.

9. At all times material to this action, Corallo owned an Apple iPhone and subscribed to Apple's iCloud cloud-storage service, which he used both for personal and business purposes.

10. NSO is an Israeli limited liability company with its principal place of business in Herzliya, Israel, and is subject to the jurisdiction of this Court.

11. Upon information and belief, NSO is a subsidiary of Q Cyber, and designs, develops, and manufactures highly invasive surveillance technology or spyware and related products and services, including the Pegasus spyware and FORCEDENTRY security exploit, which it markets, sells, distributes, operates, deploys, services and maintains for third parties around the globe, including foreign sovereign entities like Italy and the Netherlands.

12. Upon information and belief, between 2014 and February 2019, NSO obtained financing from a San Francisco–based private equity firm, which ultimately purchased a

controlling stake in NSO. In and around February 2019, NSO was reacquired by its founders and original management. NSO's annual report filed on February 28, 2019, listed Q Cyber as the only active director of NSO and its majority shareholder.

13. Q Cyber is an Israeli corporation with its principal place of business in Herzliya, Israel, and is subject to the jurisdiction of this Court.

14. Until at least June 2019, NSO's website stated that NSO was "a Q Cyber Technologies company," and NSO stated as recently as July 2021 that NSO was a subsidiary of Q Cyber. Q Cyber reportedly acts as a "commercial distributor" for NSO's products, including by signing contracts, issuing invoices, and receiving payments from NSO's customers.

15. At all times material to this action, each NSO Defendant was the agent, partner, alter ego, subsidiary, and/or coconspirator of and with the other NSO Defendant, and the acts of each NSO Defendant were in the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each NSO Defendant acted with the knowledge, permission, and consent of each other; and each NSO Defendant aided and abetted each other in their malicious activities.

16. Apple is a California corporation with its principal place of business in Cupertino, California, and is subject to the jurisdiction of this Court.

17. Apple designs, manufactures, markets, and sells smartphones, personal computers, tablets, wearables and accessories, and sells a variety of related services. iPhone is Apple's line of smartphones based on its iOS operating system. Apple's services include iCloud, a cloud-storage and cloud-computing service that enables subscribers in pertinent part to store data such as documents, photos, music and videos on remote servers for download to iOS, macOS or Windows devices.

18. Apple designed, manufactured, marketed and sold to Corallo the iPhone and iCloud storage account that was hacked by NSO Defendants which is the subject of this action.

JURISDICTION

19. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 as the cause of action arises under federal statutes, to wit, the Alien Tort Claims Act, 28 U.S.C. § 1350, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

20. This Court has supplemental jurisdiction over Plaintiff's related claims arising under California state law pursuant to 28 U.S.C. §1367(a).

21. The Court has personal jurisdiction over NSO Defendants because they obtained financing from California and directed and targeted their actions at California and consumers who purchase goods and services from California businesses, like Apple. In addition, the claims in this Complaint arise from Defendants' actions in California, tortious conduct directed and causing harm in California, systematic and continuous contact with California, including NSO Defendants' unlawful access and use of Corallo's Apple iCloud cloud storage account which is maintained on servers located in California.

22. Moreover, NSO Defendants' malicious and harmful activities brought them well within the long arm of the law and the jurisdiction of this Court, which has the authority to hold them to account for their violations of U.S. federal and California laws and for the damages they have inflicted on Plaintiff.

VENUE

23. Venue is proper in the Northern District of California pursuant to 28 U.S.C. §1391(b)(2) because all or a substantial part of the events giving rise to this action occurred in this judicial district.

DIVISIONAL ASSIGNMENT

24. Pursuant to Civil L.R. 3-2(e), this case should be assigned to San Jose Division because Apple is located in Santa Clara County, California.

GENERAL ALLEGATIONS

25. The United States as United Nations member and founder has adopted the Universal Declaration of Human Rights ("**UDHR**").[2]

26. Article 12 of the UHDR states as follows: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to protection of the law against such interference or attacks.*"

[2] The UHDR was adopted by the General Assembly in 1948.

27. The UHDR is cited as an example of the firmly established nature of privacy and integrity of "honour" in international law and the law of nations, and the right of individuals to seek redress for same. The citation also shows that the United States recognizes such rights and the right to seek redress, and that the United States recognizes that the principle is a principle of international law shared by other countries.

28. The United States also ratified the International Covenant on Civil and Political Rights ("**ICCPR**") in 1992.

29. Article 17 of the ICCPR provides as follows : "*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."*

30. In addition, Article 9 of the ICCPR states in pertinent part: "*Everyone has the right to liberty and security of person….*"

31. The Commentary in the "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework'" ("**Guiding Principles on Business and Human Rights**"), which was endorsed by the United Nations Human Rights Council in 2011, provides in relevant part as follows:

> *The responsibility of business enterprises to respect human rights is distinct from issues of legal liability and enforcement, which remain defined largely by national law provisions in relevant jurisdictions…*
>
> * * *
>
> *As a legal matter, most national jurisdictions prohibit complicity in the commission of a crime, and a number allow for criminal liability of business enterprises in such cases. Typically, civil actions can also be based on an enterprise's alleged contribution to a harm, although these may not be framed in human rights terms. The weight of international criminal law jurisprudence indicates that the relevant standard for aiding and abetting is knowingly providing practical assistance or encouragement that has a substantial effect on the commission of a crime.*
>
> *Conducting appropriate human rights due diligence should help business enterprises address the risk of legal claims against them by showing that they took every reasonable step to avoid involvement with an alleged human rights abuse. However, business enterprises conducting such due diligence should not assume*

> *that, by itself, this will automatically and fully absolve them from liability for causing or contributing to human rights abuses.*

Guiding Principles on Business and Human Rights, pp. 14, 19.

32. Article 23 of the Guiding Principles on Business and Human Rights provides:

> *In all contexts, business enterprises should:*
> *(a) Comply with all applicable laws and respect internationally recognized human rights, wherever they operate;*
> *(b) Seek ways to honour the principles of internationally recognized human rights when faced with conflicting requirements;*
> *(c) Treat the risk of causing or contributing to gross human rights abuses as a legal compliance issue wherever they operate.*

Id. at p. 25.

33. The Commentary on Article 23 of the Guiding Principles on Business and Human Rights further states:

> *Some operating environments, such as conflict-affected areas, may increase the risks of enterprises being complicit in gross human rights abuses committed by other actors (security forces, for example). Business enterprises should treat this risk as a legal compliance issue, given the expanding web of potential corporate legal liability arising from extraterritorial civil claims, and from the incorporation of the provisions of the Rome Statute of the International Criminal Court in jurisdictions that provide for corporate 26 criminal responsibility. In addition, corporate directors, officers and employees may be subject to individual liability for acts that amount to gross human rights abuses.*

Id. at pp. 25-26.

34. Corallo has had his human rights violated in contravention of the law of nations and international law by NSO Defendants in their systematic targeting, harassment, persecution, intentional infliction of emotional distress, invasion of privacy, and data hacking, as well as other offensive and actionable tortious conduct.

35. Such actions include, but are not limited to, acts of hacking Corallo's iPhone utilizing NSO Defendant technology, supervision, orchestration, data collection, and data distribution.

36. NSO Defendants designed, developed, manufactured, marketed, distributed, and operated various surveillance technology, including malware, spyware, and other hacking devices designed to secretly intercept and extract information and communications from mobile phones

and electronic devices. NSO Defendants' products included a highly invasive spyware known as "Pegasus," which NSO describes as "a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device." *See* Complaint filed in the matter of *WhatsApp Inc. and Facebook, Inc. v. NSO Group Technologies Limited and Q Cyber Technologies Limited*, No 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019) (**"WhatsApp. Complaint"**), attached as **Exhibit "A"**, Dkt 1-1 (Exhibit 10, "Pegasus – Product Description," at p. 31).

37. According to NSO, "Pegasus silently deploys invisible software ('agent') on the target device. This agent then extracts and securely transmits the collected data for analysis. Installation is performed remotely (over-the-air), does not require any action from or engagement with the target, and leaves no traces whatsoever on the device." *Id.* at p. 33. Upon successful installation of the agent, "a wide range of data is monitored and collected from the Device" including:

> **Textual:** Textual information includes text messages (SMS), Emails, calendar records, call history, instant messaging, contacts list, browsing history and more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
> **Audio:** Audio information includes intercepted calls, environmental sounds (microphone recording) and other audio recorded files.
> **Visual:** Visual information includes camera snapshots, photos retrieval and screen capture.
> **Files:** Each mobile device contains hundreds of files, some bear invaluable intelligence, such as databases, documents, videos and more.
> **Location:** On-going monitoring of the device location (Cell-ID and GPS).

Id. at p. 40.

38. Upon information and belief, from at least February 2021 until September of 2021, NSO Defendants deployed their Pegasus spyware through a security exploit they developed known as "FORCEDENTRY." *See* Complaint filed by Apple against NSO Defendants in the matter of *Apple, Inc. v. NSO Group Technologies Limited and Q Cyber Technologies Limited*, No.5:21-cv-09078 (N.D. Cal. Nov. 23, 2021) ("**Apple Complaint**"), attached as **Exhibit "B"**, ¶ 48. FORCEDENTRY is known as a "zero-click" exploit, meaning that it allows NSO Defendants to hack into the target's device without any action or awareness by the target, unlike other exploits

that require some action by the target, such as clicking a hyperlink in an email or text message. *Id.* at ¶ 49.

39. Upon information and belief, as part of the products and services provided to its clients like Italy and the Netherlands, NSO Defendants created more than one hundred Apple IDs using Apple's systems to be used in their deployment of FORCEDENTRY. Apple Complaint, ¶ 50. This was all done using Apple servers in the United States, including California. *Id.* at ¶ 51. After obtaining the Apple IDs, NSO Defendants executed the FORCEDENTRY security exploit to deploy the Pegasus spyware onto the Apple users' devices, like Corallo's iPhone, thereby infecting the devices with the spyware. *Id.*

40. According to cybersecurity research, news reports and the filings in separate litigation brought by Apple and WhatsApp against NSO Defendants, *see* Apple Complaint and WhatsApp Complaint, following the delivery of Pegasus to an Apple device like the one Corallo used, the spyware program begins transmitting personal data to a command-and-control server operated by NSO Defendants or their clients, like Italy and/or the Netherlands. *See* Apple Complaint, ¶ 52.

41. On or about November 23, 2021, Corallo received an email notification from Apple advising him that his iPhone and his iCloud account had been hacked. *See* copy of Apple's email notification attached as **Exhibit "C"**.

42. The subject of the email from Apple was titled "Alert: State-sponsored attackers may be targeting your iPhone." *Id.* The email message advised Corallo that based on Apple's belief, Corallo was being targeted by state-sponsored attackers who were trying to remotely compromise the iPhone device associated with his Apple ID. *See id.*

43. In particular, the email message from Apple advised Corallo that the "attackers are likely targeting you individually because of who you are and what you do." *Id.* The email advised Corallo that, "[i]f your device is compromised by a state-sponsored attacker, they may be able to remotely access your sensitive data, communications, or even the camera and microphone," and warned him that "[w]hile it's possible that this is a false alarm, please take this warning seriously." *Id.*

44. Apple recommended that Corallo update his iPhone to the latest software version, *see id.*, which Corallo promptly did. Corallo also signed out of all messaging and cloud services, and restored his device to factory settings, and then promptly purchased a new iPhone to use.

45. Apple also recommended that Corallo enlist the aid of a cybersecurity expert to assess the extent of the data breach and to help him with a rapid-response to NSO Defendant's cyberattack, and further recommended that Corallo be cautious with all future links he received via email. *See id.*

46. Unfortunately, Apple's after-the-fact and late warning to Corallo was not a false alarm. As confirmed by forensic analysis, Corallo was the target of a cyberattack and hacking by NSO Defendants.

47. When Corallo chose to purchase his Apple iPhone device and subscribe to Apple's iCloud storage service, he did so because he trusted Apple's reputation as the best in class – touted by Apple as one of the safest and most secure mobile device on the market with "powerful" security features to prevent anyone but the owner/user from accessing data on the iPhone and iCloud account. *See e.g.,* https://support.apple.com/guide/iphone/use-built-in-security-and-privacy-protections-iph6e7d349d1/ios ("iPhone is designed to protect your data and your privacy. Built-in security features help prevent anyone but you from accessing the data on your iPhone and in iCloud."); https://support.apple.com/en-us/HT202303 ("iCloud uses best-in-class security technologies, employs strict policies to protect your information, and leads the industry by adopting secure, privacy-preserving technologies like end-to-end encryption for your data.").

48. The potential for a cyberattack on Apple's customers by NSO Defendants was known or should have been known by Apple. Prior to the hacking incident by NSO Defendants in this case, Apple had already experienced hacking incidents involving NSO Defendants and was well aware that its devices and iCloud storage accounts were highly susceptible to hacking by NSO Defendants. Apple's knowledge of the threat posed by NSO Defendants and the extent of the data breach capabilities (and the harm already inflicted on Apple and its customers) is highlighted in the separate lawsuit brought by Apple against NSO Defendants. *See* Apple Complaint.

49. Despite actual knowledge of NSO Defendants' hacking capabilities and their actual

past cyberattacks directed towards Apple and its customers, prior to the hacking incident by NSO Defendants in this case, Apple did not warn Corallo that he was a target of NSO Defendants' hacking campaign or that their products and services were highly susceptible to hacking by NSO Defendants.

50. Other than the generic and seemingly form email notification (sent after the hacking incident by NSO Defendants in this case), *see* Exhibit "C", Apple did not provide Corallo with any other advice or direct assistance to actually deal with the repercussions of NSO Defendants' hacking of Carollo's Apple iPhone and iCloud account.

51. NSO Defendants' actions, along with Apple's negligence and false or misleading advertising, have injured, harmed, and have caused damages to Plaintiff actionable under federal and state law.

COUNT I – VIOLATION OF THE ALIEN TORT CLAIMS ACT
28 U.S.C. § 1350
(AGAINST NSO DEFENDANTS)

52. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

53. The Alien Tort Claims Act ("**ATA**") provides redress for claims involving aliens who have committed torts in violation of the law of nations (international law) or a treaty of the United States.

54. Universally accepted norms of the law of nations and international law prohibit systematic abuse of human rights, which includes acts of targeting, harassment, persecution, intentional infliction of emotional distress, as well as acts of invasion of privacy, as enshrined in the UDHR.

55. The aforementioned monitoring, surveillance, and hacking of Corallo's iPhone constitutes actionable acts under the ATA for the torts of invasion of privacy.

56. The intentional actions aforementioned of invasion of privacy have harmed Corallo in an amount to be proven at trial, and which may allow him to claim punitive damages due to their egregious conduct.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive

damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct actionable under the ATA.

COUNT II – VIOLATIONS OF THE FEDERAL COMPUTER FRAUD AND ABUSE ACT 18 U.S.C. § 1030 (AGAINST NSO DEFENDANTS)

57. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

58. Corallo is an Apple user. His devices are his subscriptions to Apple iPhone device and iCloud. His iPhone is a "computer" as described by the Computer Fraud and Abuse Act, 18 U.S.C. §1030(e)(1).

59. Corallo's iPhone is a "protected computer" as defined by 18 U.S.C. §1030(e)(2)(B) because it is "used in or affecting interstate commerce or communications" in the United States.

60. NSO Defendants violated and attempted to violate 18 U.S.C. § 1030(a)(2) because they intentionally accessed and attempted to access the iOS operating system in Corallo's iPhone and his iCloud account without authorization and, upon information and belief, obtained information from Corallo's iPhone and iCloud account belonging to Plaintiff.

61. NSO Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with the intent to defraud accessed the operating system on Corallo's iPhone without authorization using information from the Apple's servers and then installed highly invasive spyware on Corallo's iPhone and by means of such conduct furthered the intended fraud and obtained information about Plaintiff illegally. This access was without authorization from Plaintiff or from Apple.

62. As a result of the fraud NSO Defendants obtained something of extreme value: financial and confidential and privileged information and communications between Plaintiff and others, including information and communications concerning Corallo's businesses, close business associates and his attorneys.

63. NSO Defendants' actions caused Plaintiff to incur a loss as defined by 18 U.S.C. §1030(e)(11), in an amount in excess of $5,000.00 during a one-year period, including the expenditure of resources to investigate and remediate NSO's illegal conduct. Plaintiff is entitled to compensatory damages in an amount to be proven at trial, as well as injunctive relief or other

equitable relief in accordance with 18 U.S.C. §1030(g).

64. NSO Defendants violated 18 U.S.C. § 1030(a)(5)(A) because they knowingly caused the transmission of a program, information, code, and/or command, specifically the commands needed to carry out the exploits described above, as well as Pegasus spyware itself, to Apple's servers, and as a result of such conduct intentionally caused damage without authorization to the operating system in Corallo's Apple devices, including by installing the Pegasus spyware.

65. NSO Defendants violated 18 U.S.C. §1030(a)(5)(B) because they intentionally accessed Corallo's Apple device without authorization and as a result of such conduct, recklessly caused damage to the operating system on Corallo's Apple device, including by installing the Pegasus spyware.

66. NSO Defendants violated 18 U.S.C. §1030(a)(5)(C) because they intentionally accessed Corallo's Apple device and iCloud account without authorization and as a result of such conduct, recklessly caused damage to the operating system on Corallo's Apple device, including by installing the Pegasus spyware.

67. NSO Defendants violated 18 U.S.C. §1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

COUNT III – INVASION OF PRIVACY
CALIFORNIA STATE LAW
(AGAINST NSO DEFENDANTS)

68. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

69. NSO Defendants engaged in conduct that was not consented to by Plaintiff.

70. NSO Defendants caused a harm to Plaintiff with the acts described herein, which constitute an intentional invasion of Plaintiff's rights to privacy.

71. The invasion, as described herein, was concrete and particularized, actual and imminent, not conjectural or hypothetical.

72. The injury arising from the acts complained of herein, has deeply affected Plaintiff in a personal and individual way and Plaintiff does not have to show any pecuniary harm at this point considering that invasion of privacy in and of itself constitutes an intentional tort on the part of NSO Defendants as described herein.

73. NSO Defendants intentionally intercepted the contents of Plaintiff's electronic communications using a device in violation of the Wiretap Act, 18 U.S.C. §2511(2)(d) since NSO Defendants were not parties to the conversation and Plaintiff would have never given consent to the interceptions.

74. NSO Defendants also harmed Plaintiff with their invasion of privacy by their violations of the Computer Fraud and Abuse Act as alleged in COUNT ONE of this Complaint.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

COUNT IV – CIVIL CONSPIRACY
CALIFORNIA STATE LAW
(AGAINST NSO DEFENDANTS)

75. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

76. Plaintiff was harmed by NSO Defendants and were all responsible for the invasion of privacy, interference with Plaintiff's possessory interest in the iPhone device, and all violations under 18 U.S.C. §1030 because NSO Defendants were all part of the overarching scheme to intentionally access Corallo's Apple device and intercept the contents of Plaintiff's iPhone.

77. A conspiracy is an agreement by two or more persons to commit a wrongful act. Such an agreement may be made orally or in writing or may be implied by the conduct of the parties.

78. If it is found that NSO Defendants committed the invasion of privacy, interference with Plaintiff's possessory interest in the iPhone device, and all violations under 18 U.S.C. §1030 that harmed Plaintiff's, then it must be determined each of NSO Defendants responsibility for the harm.

79. All NSO Defendants were aware of the invasion of privacy, interference with Plaintiff's possessory interest in the iPhone device, and all violations under 18 U.S.C. §1030 and each agreed and intended that such torts be committed upon Plaintiff.

80. NSO Defendants' actions caused Plaintiff to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate NSO Defendants' conduct, damage to Plaintiff's reputation, and damage to the relationships and goodwill of Plaintiff's businesses. Plaintiff has been damaged in an amount to be proven at trial.

WHEREFORE, Plaintiff respectfully request this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

COUNT V – NEGLIGENCE
CALIFORNIA STATE LAW
(AGAINST APPLE)

81. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

82. Apple owed a duty to Plaintiff to protect all data of the cloud storage including sensitive material of Plaintiff.

83. Apple's failed to prevent and/or adequately and reasonably defend against the hacking by NSO Defendants despite Apple's knowledge that NSO Defendants were actively targeting its customers with their malware and spyware and other surveillance technology, and for falsely advertising its ability to prevent such cyberattacks.

84. Plaintiff was injured as a proximate, direct, and foreseeable result of Apple's negligence.

85. Apple was negligent as NSO Defendants accessed Corallo's Apple device without authorization and as a result of such conduct, recklessly caused damage to the operating system on Corallo's Apple device, including by installing the Pegasus spyware, without any protection from the Apple device.

86. Plaintiff is entitled to an award of damages due to Apples negligence that allowed NSO Defendants to access Corallo's Apple device without authorization and as a result of such

conduct, recklessly caused damage to the operating system on Corallo's Apple device, including by installing the Pegasus spyware.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against Apple for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of Apple's negligent conduct.

COUNT VI – VIOLATIONS OF CALIFORNIA'S COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CAL. PENAL CODE § 502 (AGAINST NSO DEFENDANTS)

87. Plaintiff re-alleges the allegations of paragraphs 1 through 51, above.

88. NSO Defendants knowingly accessed and without permission altered and used Plaintiff's data contained on Corallo's Apple iPhone and iCloud storage accounts (which are maintained on servers located in California) in order to: (a) devise and execute a scheme and artifice to defraud and deceive, and (b) wrongfully control and obtain money, property, and data in violation of California Penal Code § 502(c)(1).

89. NSO Defendants knowingly and without permission used and caused to be used Apple's servers, including servers located in California, in violation of California Penal Code § 502(c)(3).

90. NSO Defendants knowingly and without permission provided and assisted in providing a means of accessing Plaintiff's computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(6).

91. NSO Defendants knowingly and without permission accessed and caused to be accessed Plaintiff's computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(7).

92. NSO Defendants knowingly introduced a computer contaminant into Plaintiff's computers, computer systems, and computer networks in violation of California Penal Code § 502(c)(8).

93. NSO Defendants' actions caused Plaintiff's to incur losses and damages, including, among other things, the expenditure of resources to investigate and remediate Defendants'

conduct, damage to Plaintiff's reputation, and damage to the relationships and goodwill between Plaintiff and his businesses customers. Plaintiff has been damaged in an amount to be proven at trial.

94. Because Plaintiff suffered damages and a loss as a result of Defendants' actions and continues to suffer damages as result of Defendants' actions, Plaintiff is entitled to compensatory damages, attorneys' fees, and any other amount of damages to be proven at trial, as well as injunctive relief under California Penal Code §§ 502(e)(1) and (2).

95. Because Defendants willfully violated California Penal Code § 502, and there is clear and convincing evidence that Defendants acted with malice and oppression and committed "fraud" as defined by section 3294 of the Civil Code, Plaintiff is entitled to punitive and exemplary damages under California Penal Code § 502(e)(4).

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

COUNT VII – VIOLATIONS OF CALIFORNIA'S FALSE ADVERTISING LAW CAL. BUS. AND PROF. CODE, §§ 17500 *ET SEQ.* (AGAINST APPLE)

96. Corallo re-alleges the allegations of paragraphs 1 through 51, above.

97. Apple's representations in connection with the sale of the iPhone and iCloud subscriptions to Corallo that were one of the safest and most secure mobile device on the market with "powerful" security features that would prevent anyone but the owner/user from accessing data on the iPhone and iCloud account and that iPhone and iCloud were designed to protect Corallo's data with built -in security features, were and are false and misleading within the meaning of California's False Advertising Law (California Business and Professional Code, § 17500) because, *inter alia*, Apple did not disclose that the iPhone and iCloud account were susceptible to hacking by hackers like NSO and foreign sovereigns through their use of NSO's Pegasus spyware and FORCEDENTRY security exploit.

98. These representations were communicated to Apple consumers, like Corallo,

because they were included in and formed a key part of Apple's advertising and marketing campaigns used to coerce potential consumers to buy its products and services, including the iPhone and iCloud storage. The representations made by Apple in its advertising were actually false and/or misleading because Apple's security features were not in fact "powerful" but highly susceptible to hacking by NSO which Apple knew as demonstrated by lawsuits filed by Apple and other technology companies. *See Apple, Inc. v. NSO Group Technologies Limited and Q Cyber Technologies Limited*, No.5:21-cv-09078 (N.D. Cal. Nov. 23, 2021); *WhatsApp Inc. and Facebook, Inc. v. NSO Group Technologies Limited and Q Cyber Technologies Limited*, No 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019). Apple's statements and misrepresentations regarding its security features would have a tendency to mislead or deceive a reasonable consumer and did deceive and mislead Corallo.

99. Corallo relied on these misrepresentations when he purchased his iPhone and subscribed to Apple's iCloud storage account.

100. Corallo was harmed as a proximate, direct, and foreseeable result of Apple's false or misleading statements in connection with Apple's sale of the iPhone and iCloud subscriptions to Corallo. Had Apple disclosed that NSO could infect Corallo's Apple iPhone device and iCloud account with NSO's Pegasus spyware or that NSO had been targeting Apple users on behalf of foreign sovereignties, Corallo not have purchased the device and subscribed to Apple's iCloud service.

101. Apple's false or misleading statements alleged herein amount to false advertising within the meaning of California's False Advertising Law, California Business and Professions Code, §17500 *et seq.*

102. Apple continues to make the same false or misleading statements with respect to its iPhone and iCloud cloud storage service, such that, unless it is enjoined from doing so, Corallo will continue to be harmed because his data is still protected as advertised. Corallo has continued to pay for iCloud services and is concerned about the fate of information contained on his iPhone and iCloud stored data given Corallo's recent discovery of NSO's activities. Corallo therefore is entitled to and pray for an injunction to, inter alia, prevent Apple from continuing to disseminate

these false and misleading statements.

103. Apple has been able to and has charged a price premium for its iPhone and iCloud subscription service by representing falsely that it has "powerful" security features.

104. Pursuant to California Business and Professions Code, §17535, Corallo is entitled to and seek an order of restitution for moneys paid by Corallo to Apple for his iPhone and iCloud subscription.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

COUNT VIII – INTENTIONAL INFLICT OF EMOTIONAL DISTRESS CALIFORNIA STATE LAW (AGAINST NSO DEFENDANTS)

105. Corallo re-alleges the allegations of paragraphs 1 through 51, above.

106. NSO Defendants' aforementioned conduct involving hacking, surveillance, and data theft of Corallo's iPhone device constitutes outrageous and actionable conduct.

107. NSO Defendants' aforementioned involving hacking, surveillance, and data theft of Corallo's iPhone device had the intention or had reckless disregard of causing emotional distress.

108. Corallo has suffered severe or extreme emotional distress as a result of NSO Defendants' aforementioned conduct of hacking, surveilling, and data theft of Corallo's iPhone device.

109. NSO Defendants' aforementioned conduct of hacking, surveilling, and data theft of Corallo's iPhone device is the proximate cause of the emotional distress suffered by Corallo.

WHEREFORE, Plaintiff respectfully requests this Court enter judgment against NSO Defendants for all damages suffered by Plaintiff, including compensatory damages, punitive damages, interest, attorney's fees and costs, and any other remedies (monetary and/or equitable) allowable by law as a result of NSO Defendants' unlawful conduct.

Dated: September 13, 2022

OSORIO INTERNACIONAL, P.A.

/s/ *Carlos F. Osorio*
Carlos F. Osorio (*pro hac vice admission pending)*
Attorneys for Plaintiff Francesco Corallo

DEMAND FOR JURY TRIAL

Plaintiff Francesco Corallo demands a jury trial as provided by Rule 38 of the Federal Rules of Civil Procedure.

Dated: September 13, 2022

OSORIO INTERNACIONAL, P.A.

/s/ *Carlos F. Osorio*
Carlos F. Osorio (*pro hac vice admission pending)*
Attorneys for Plaintiff Francesco Corallo